Livermore Computing Computer Security Briefing

Please read and mail or fax a signed copy of this document to LC Customer Service Group
Lawrence Livermore National Laboratory, PO Box 808 L-63, Livermore CA 94551 •Fax (925) 422-0592

This is a list of general computer use policies and security rules that apply to **all off-site users** requesting access to Livermore Computing (LC) unclassified computer resources. Off-site users of LC resources are **required** to submit a signed copy of this document and its appendix *Briefing on Sensitive Unclassified Information and Protecting Unclassified Computer Systems and Information* **before** obtaining their unclassified computer account at LC.

The United States government for the purpose of supporting the Laboratory's programmatic and business activities funds Lawrence Livermore National Laboratory (LLNL) computer communications systems. These government resources are to be used for official business only. LLNL personnel in LC Customer Services and Support or in Computer Security or an agent of the federal government may at any time and without notice audit or access any LLNL computer communications system. Any information obtained through such auditing or access may be disclosed within LLNL and to outside parties, including law enforcement authorities.

Computers and network systems are inherently insecure. Protect sensitive information and applications accordingly.

Non-LLNL employees

Computer communications systems provided by LLNL are to be used only for work-related purposes (as determined by the responsible manager). The use of this equipment or software for personal or non-work-related activity is prohibited. User Accountability: Users face administrative or criminal sanctions for unauthorized use of LLNL computer communications systems.

Unauthorized Access

Users are not to access or attempt to access systems or information for which they are not authorized. Users are not to attempt to receive unintended messages or access information by some unauthorized means, such as imitating another system, impersonating another user or other person, misuse of legal user credentials (user names, passwords, etc.), or by causing some network component to function incorrectly. Users are not to possess or transfer information for which they are not authorized.

Passwords and User Names

A user identifier (name or employee number) known as a User Name and password are required of all users of a multi-user system (two or more users) or of a system allowing any access through a network or telephone line (modems). Passwords must be protected commensurate (equal) to the data and system they protect. Passwords must be changed at least biannually. Passwords must be at least six (6) characters long, not found in a dictionary, and cannot be the name of a person, place, or thing. Passwords must not be shared with any other person. The password must be changed as soon as possible after an unacceptable exposure or suspected compromise. Sharing of passwords is considered a serious offense and would result is loss of access privileges to LC computer systems.

Malicious Software:

Users must not introduce or use malicious software such as computer viruses, Trojan horses, or worms.
Altering Authorized Access: Users are prohibited from changing access controls to allow themselves or others to perform actions outside their authorized privileges.

Denial of Service Actions:

Users are not allowed to prevent others or other systems from performing authorized functions by actions that deny their access, their communications capability, deliberately suppressing their messages or generating frivolous or unauthorized traffic.
Data Modification or Destruction: Users are prohibited from taking unauthorized actions to intentionally modify or delete information or programs.
Reconstruction of Information or Software: Users are not allowed to reconstruct or recreate information or software for which they are not authorized.

Misuse, Abuse, and Criminal Activity

All LLNL personnel, organizations, subcontractors, and remote users are to report potential LLNL computer communications systems misuse, abuse, and criminal activities to the LC Customer Services and Support Group. You are required to read the Appendix to this document, *Briefing on Sensitive Unclassified Information and Protecting Unclassified Computer Systems and Information*, **before** you submit your completed form.

If you are unwilling to abide by this computer use policy and security rules, do not apply, or use, LLNL computer communications systems.

Acknowledgement of Terms and Conditions

I have read the LC Computer Security Briefing for Off-site Users and *Briefing on Sensitive Unclassified Information and Protecting Unclassified Computer Systems and Information*. I agree to abide by the requirements set forth in this document when using LC/LLNL computing resources		
Last Name	First Name	Middle Initial
Unclassified E-mail	Citizenship (if not U.S., include VTS/Fast Track numbers)	
User Signature	Date	
Principal Investigator Name		

Mail or fax completed forms to LC Customer Service Group
Lawrence Livermore National Laboratory, PO Box 808 L-63, Livermore CA 94551 • Fax (925) 422-0592
Questions? Contact the LC Customer Service Group by phone at (925) 422-4531, Option 2 or send e-mail to lc-support@llnl.gov

Briefing on Sensitive Unclassified Information and Protecting Unclassified Computer Systems and Information*

***Also known as Unclassified Controlled Information (UCI).**

Definition of Sensitive Unclassified Information (SUI)

Government. Other government interests are those related, but not limited to, the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law-enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided the U.S. Government by its citizens. Information found within the automated data processing (ADP) system and its associated telecommunications system clearly falls into this category (as defined in U.S. DOE Order 5639.1).

Sensitive Information is described as information, the disclosure of which could reasonably be expected to adversely affect national or DOE security interests. This includes both classified and unclassified information and matter (e.g., Export Controlled Information, Naval Nuclear Propulsion Information, Unclassified Controlled Nuclear Information, Official Use Only Information, and certain unclassified information, or matter) as identified in program Critical and Sensitive Information Lists.

Categories of Sensitive Unclassified Information (SUI):

- Unclassified Controlled Nuclear Information (UCNI)
- Export Controlled
- Mission Essential Unclassified Information
- Official Use Only (OUO)
- Privacy Protected Information
- Business Protected Information
- Sensitive Subjects (LLNL)
- Anything defined by program management as sensitive

Additional Information on SUI:

- Computer Security Organization document CSG2315.
- DOE Guidance on determining whether information is sensitive.

Note: These documents are available from LLNL's Computer Security Program office.

Protecting Unclassified Computer Systems and Information

Users Must Be Aware of the Following:

- All users must employ secure password practices.
  - Hackers are very good at stealing clear text passwords as you log in from a remote site (ISP, University, @Home, etc.).
  - Do not log in to LLNL computers via the Internet unless you protect your password.
  - Use a "one-time-password."
  - Use an encrypted password (e.g., SSH).
- E-mail is not secure--it is not even private.
  - E-mail is more like a post-card than a letter--it is easy to snoop.
  - E-mail servers sometimes make mistakes and your e-mail may go to places it was never intended.
  - If you send (unencrypted) sensitive data via e-mail--you are putting that data at risk.
- Sending SUI over a network
  - SUI should be encrypted when it is sent over the Internet.
  - Media containing SUI should be clearly labeled.
- Protecting Media
  - Media containing SUI should be locked in a desk or cabinet when unattended.
  - Media can be locked in an office.
- Clearing Sensitive Unclassified Media
  - To truly (electronically) erase information, you must use a program that overwrites the data at least three times
  - Simply "deleting" sensitive unclassified files is NOT sufficient.
  - Putting a file in the Macintosh Trash can and emptying the trash is NOT enough.
  - Deleting a file on a PC or putting it in the Recycle Bin and emptying the Recycle Bin on a Windows computer is NOT enough.
  - Removing a file (rm) on a Unix computer is NOT enough.
  - Reformatting the disk is NOT sufficient.

Encryption

- LLNL Computer Security Organization recommends that you use encryption to protect sensitive unclassified information (SUI).
- Encryption scrambles the data so it is unintelligible unless you have the key that was used to encrypt the data.
- Put a copy of your encryption key (password/pass phrase) in a sealed envelope. Store the envelope in a secure repository or vault. Your encryption key would then be available in case of emergency.

Encryption Products

- For Macintosh to Macintosh exchanges, the freeware program Curve Encrypt works well. It is available from: CS Public: Software: Encryption Freeware-Mac: Curve Encrypt 2.2.sea (Note: You need Stuffit Expander to uncompress this freeware.) It can be used to protect data on the disk and over the network.
- If you need to share encrypted data with users on other computers (other than Macintosh), the freeware program Pretty Good Privacy (PGP) works.
  - It can be used to protect data on the disk and over the network.
  - PGP at this time does not have a user friendly interface and it requires an ad hoc key infrastructure.
- You can use SSH (Secure Shell) to access Livermore Computing computer communications systems.
  - With SSH, all the data exchanged between the client (Mac/PC/UNIX) and the host (UNIX) is encrypted. SSH does not protect the data.
  - SSH only protects data over the network, not on the disk.

Mail or fax completed forms to LC Customer Service Group

Lawrence Livermore National Laboratory, PO Box 808 L-63, Livermore CA 94551 • Fax (925) 422-0592

Questions? Contact the LC Customer Service Group by phone at (925) 422-4531, Option 2 or send e-mail to lc-support@llnl.gov